Problème 8

Un polynôme P de degré $n \geqslant 1$ est dit antisymétrique si $P(-x) = x^n P(\frac{1}{x})$ pour tout nombre réel non nul x. Montrer qu'un polynôme antisymétrique avec des coefficients entiers impairs n'a pas de racine sur le cercle unité de $\mathbb{C}$.

Solution de l'auteur : En écrivant

$$P(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

on déduit de l'antisymétrie les relations

$$a_{n-k} = (-1)^k a_k \quad \text{pour tout} \quad k = 0, \ldots, n. \tag{20}$$

En particulier, $a_n = a_0 = (-1)^n a_n$; comme $a_n \neq 0$, on en déduit que n est pair.

Ensuite, nous avons $a_{n/2} = (-1)^{n/2} a_{n/2}$; comme $a_{n/2} \neq 0$, on en déduit que $n/2$ est aussi pair. On a donc $n = 4m$ avec un entier m strictement positif.

En raisonnant par l'absurde, supposons qu'il existe une racine u du module un de P. Alors, en utilisant (20), l'égalité suivante a lieu :

$$0 = u^{-2m} P(u) = a_{2m} + \sum_{j=1}^{m} a_{2m+2j}(u^{2j} + u^{-2j}) + \sum_{j=1}^{m} a_{2m+2j-1}(u^{2j-1} - u^{-2j+1}). \tag{21}$$

Comme la première somme est réelle et la seconde est purement imaginaire, on a nécessairement

$$a_{2m} + \sum_{j=1}^{m} a_{2m+2j}(u^{2j} + u^{-2j}) = \sum_{j=1}^{m} a_{2m+2j-1}(u^{2j-1} - u^{-2j+1}) = 0,$$

d'où u est une racine commune des polynômes

$$Q(z) := \sum_{j=0}^{2m} a_{2j} z^{2j} \quad \text{et} \quad R(z) := \sum_{j=1}^{2m} a_{2j-1} z^{2j-1}.$$

Par conséquent, ils ont un commun diviseur $M(z)$ de degré ≥ 1 : le polynôme minimal de u.

En choisissant M tel que le plus grand commun diviseur de ses coefficients soit égal à 1, son coefficient principal est impair, donc $\deg M \geq 1$, même si M est considéré comme un polynôme à coefficients dans le corps $\mathbf{F}_2 := \{0, 1\}$ à deux éléments.

Comme polynômes dans $\mathbf{F}_2[z]$, Q et R s'écrivent sous la forme

$$Q(z) = \sum_{j=0}^{2m} z^{2j} \quad \text{et} \quad R(z) = \sum_{j=1}^{2m} z^{2j-1}.$$

Par conséquent, $M(z)$ divise $zR(z) - Q(z) = 1$, contradisant la relation $\deg M \geq 1$.

Remarque. *Une fin de preuve alternative, sans utiliser le corps $\mathbf{F}_2[z]$ a été proposée par Pàl Péter Pàlfy : Comme u est une racine de $Q(z)$ et de $R(z)/z$, il est aussi une racine de $Q(z) + R(z)/z$ et de $Q(z) - R(z)/z$. Leur coefficient principal est impair, les autres sont pairs, et le terme constant d'un des deux n'est pas un multiple de 4. Celui-ci est le polynôme minimal de u d'après le critère de Schönemann–Eisenstein. Mais il ne peut pas être un diviseur de $R(z)/z$, parce que le degré du dernier est plus petit. Cette contradiction prouve le résultat cherché.*

Solution de l'équipe Tigré : Soit P un polynôme antisymétrique à coefficients impairs. Supposons par l'absurde que P admet une racine z de module 1.

On a :

$$\begin{aligned} P(X) &= (-X)^{\deg P} P\left(-\frac{1}{X}\right) \\ &= (-X)^{\deg P} \left(\frac{1}{X}\right)^{\deg P} P(X) \\ &= (-1)^{\deg P} P(X). \end{aligned}$$

Ainsi, comme P est non identiquement nul, il est de degré pair, qu'on notera $2n$.

Notons $Q := (P(X) + P(-X))/2$ et $R := (P(X) - P(-X))/2$. Les polynômes Q et R sont respectivement pair de degré $2n$ et impair de degré $2n-1$. De plus $P = Q + R$, et donc :

$$Q(z) + R(z) = 0.$$

Or z est de module 1, et P antisymétrique à coefficients réels, et donc :

$$\begin{aligned} P(-z) &= P\left(-\frac{1}{\overline{z}}\right) \\ &= \frac{1}{\overline{z}^n} P(\overline{z}) \\ &= \frac{1}{\overline{z}^n} \overline{P(z)} \\ &= 0. \end{aligned}$$

Donc $-z$ est également une racine de P, ainsi $Q(z) - R(z) = 0$. On en déduit que z est une racine commune de $Q + R$ et $Q - R$, puis que z est à la fois une racine de Q et de R.

Or Q et $X^{-1}R$ sont deux polynômes pairs (au sens où leurs coefficients d'indices impairs sont nuls), dont les coefficients d'indices pairs sont impairs, car ceux-ci font partie de la suite des coefficients de P. Autrement dit, il existe deux polynômes $\tilde{Q}$ (de degré n) et $\tilde{R}$ (de degré $n-1$) à coefficients impairs vérifiant :

$$Q(X) = \tilde{Q}(X^2) \text{ et } X^{-1}R(X) = \tilde{R}(X^2).$$

En évaluant ces égalités en z, on voit que z^2 est une racine commune à $\tilde{Q}$ et $\tilde{R}$.

Par ailleurs, l'imparité des coefficients s'écrit :

$$\tilde{Q} \equiv \sum_{k=0}^{n} X^k \ [2] \text{ et } \tilde{R} \equiv \sum_{k=0}^{n-1} X^k \ [2].$$

Donc on peut écrire (les résultants étant considérés dans $\mathbb{Z}[X]$) d'une part :

$$\operatorname{Res}(\tilde{R}, \tilde{Q}) \equiv \operatorname{Res}\left(\sum_{k=0}^{n-1} X^k, \sum_{k=0}^{n} X^k\right) \ [2]$$

(il suffit de passer modulo 2 matriciellement, coefficient par coefficient)

Et d'autre part :

$$\begin{aligned} \operatorname{Res}\left(\sum_{k=0}^{n-1} X^k, \sum_{k=0}^{n} X^k\right) &= \prod_{k=1}^{n-1} \prod_{l=1}^{n} \left(e^{\frac{2ik\pi}{n}} - e^{\frac{2il\pi}{n+1}}\right) \\ &= \prod_{k=1}^{n-1} \sum_{l=0}^{n} \left(e^{\frac{2ik\pi}{n}}\right)^l \\ &= \prod_{k=1}^{n-1} \frac{e^{\frac{2ik(n+1)\pi}{n}} - 1}{e^{\frac{2ik\pi}{n}} - 1} \\ &= 1, \end{aligned}$$

Ainsi, le résultant $\mathrm{Res}(\tilde{R}, \tilde{Q})$ est impair, en particulier il est non-nul. Donc $\tilde{Q}$ et $\tilde{R}$ n'ont pas de racine commune. Ce qui nous donne la contradiction voulue.